EXHIBIT 4

EnCase Enterprise Edition

This Product Review is in the following Category:
Security Management, Assessment, Incident Response

This Product Review is in the following Sub-category:
IT Forensics

Version: 4.09
Vendor: Guidance Software
Website: www.guidancesoftware.com
Price: from $25,000
Date: 1-Jan-03
Author: Jon Tullett

EnCase from Guidance Software has established itself as the leading tool for forensic investigators. Perceiving a need for similar tools in the enterprise space, the company announced EnCase Enterprise Edition, bringing most of the functionality enjoyed by criminal forensic investigators to corporate users.

In its forensic version, EnCase exists to capture, analyze and report on data so that investigators can manage electronic evidence in specific cases. In a corporate world, this becomes more of a real-time job, serving the ongoing purposes of incident response and auditing in addition to forensic tasks.

The forensic edition (which SC Magazine has reviewed in the past) does an excellent job of analyzing and managing evidence. In the network-aware enterprise version, there's little functional change, but the acquisition and processing of forensic data can be conducted on remote systems, even while they are running live.

This is accomplished by installing 'servlets' on the remote systems. These run on Windows systems (Linux variants are under development following customer demand, Guidance says) and provide extensive access to the PC's mounted volumes, including CDs, floppy disks, Palm handhelds (not yet Pocket PC or Symbian), and file systems of almost any sort, including Unix and Macintosh formats.

The investigator runs the EnCase examiner front-end, which is very similar to the forensic edition, and establishes a connection to the remote servlet. To avoid abuse, this is done via a proxy, a key management server which authenticates the investigator and instructs the servlet to allow access. The key hierarchy is tightly controlled by Guidance - lose the master key and you'll have to endure a lengthy and stringent process to recover it. That may be a chore, but it's worthwhile: any compromise of your key server and you'll turn that fancy forensic suite into a deployment of backdoor Trojans.

The client software requires a dongle to operate, providing another layer of security. Guidance takes pains to ensure that the product will not be misused, and the product training and documentation goes to some lengths to indicate best-practice procedures. Both training and documentation are excellent; well thought out and lucid.

Besides controlling access, each administrator can be assigned specific roles and tasks, restricting their rights on sensitive cases.

The forensic edition of the product works by acquiring data from the target system and then analyzing it on the examiner's PC; the enterprise version can also examine data in situ. This is a very powerful feature - it allows routine checks for forbidden material or IP violations to happen in the background, or for preliminary investigations into a possible incident to be conducted without fanfare.

Data analysis is comprehensive, and getting better with every edition of the product. Standard issue features like binary and hex dumps of disk space, including unallocated space and clusters that are marked bad, are all present and correct. Some standard activities that examiners will do frequently, like searching for image files, are automated - the front-end provides a neat thumbnail gallery of image files in a specified location. The pattern-matching and searching is excellent, using POSIX-like regular expressions on any data. A powerful script engine provides support for custom-written add-ons, which will particularly appeal to users wanting to ensure compliance to specific policies.

Complex file types, such as Outlook folders or compressed archives, can be opened and explored, often in defiance of password protection. With many of these files 'security' is really for show, and EnCase is able to bypass some. There are some notable gaps, such as a lack of support for Microsoft web archives, but more are being added all the time. Guidance has a good track record of responding to customer requests for new features, so it's likely issues such as these will be addressed rapidly if there is sufficient need.

License fees for EnCase are calculated by the number of investigator client seats, not the number of servlets, meaning you can roll out the connectors through the entire enterprise without incurring extra cost, and only purchase investigator licenses when the need arises.

Despite doing intensive tasks on the evidence systems, the performance overhead is usually negligible. The network performance will spike if you remotely mirror an entire drive, and the user is likely to notice spontaneous floppy drive activity, but most scan-and-retrieve activities are unlikely to be noticed.

Looking closely at the product, it's obvious that anyone who really knows what they're doing will be able to hide information from an investigator, though not every black hat is going to be intimately familiar with EnCase or any other forensic product. There are far too many clever places to conceal data, even large quantities of it. But the challenge here is different to that facing a criminal forensic expert, who needs to find the data itself: just finding traces of that activity may be enough for a corporate officer to take action and launch a more thorough investigation.

This is not a tool for casual scanning of PCs or for day-to-day desktop monitoring, giving it possibly a more limited appeal in

corporate environments. But as a forensic tool with specific purposes, EnCase is unsurpassed

Products Homepage Browse Products

RELATED PRODUCT REVIEWS IN THIS SUBCATEGORY
NetSwift iGate
LapTrak (Mobile Security group test)
Magi Enterprise (Telecommuting group test)
eTrust Intrusion Detection (IDS group test)
Symantec Client Security (Telecommuting group test)
more ...